

Week- 5: Network Security in the Cloud

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

College Name- Sanjivani University

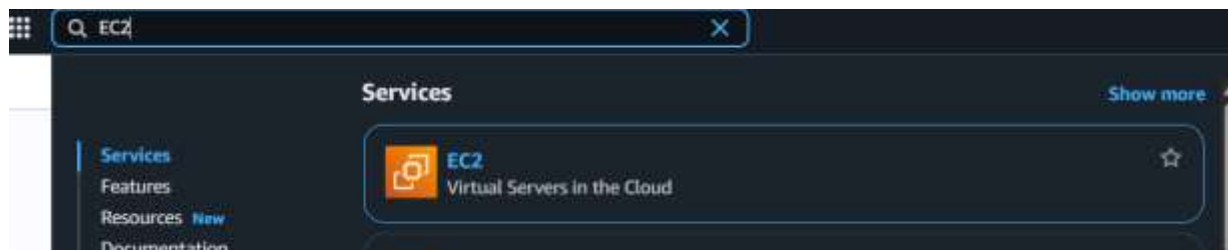
Email ID- samruddhi.nikam_24ucs@sanjivani.edu.in

- ❖ TASK- 1) Configure security groups and firewall rules.
2) Block unnecessary ports.
3) Document security ruleset.

🔧 Configure security groups and firewall Rules.

Step 1- Log in to AWS Console, Go to <https://aws.amazon.com>, Sign in to the AWS Management Console

Step 2- Open the EC2 Dashboard, In the AWS Console, search for **EC2** in the services.



Step 3- Click on Security Groups in the left sidebar under "Network & Security"



Week- 5: Network Security in the Cloud

Step 4- Create a Security Group, fill the details of security groups.

EC2 > Security Groups > Create security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name

security_group

Name cannot be edited after creation.

Description

first security group

VPC

vpc-0b963cf2f9cf92e16

Step 5- Then Enter the Inbound and outbound Rules and click create group button.

Inbound rules

Type

SSH

Protocol

TCP

Port range

22

Source

M

47.11.10.18/32

Description - optional

Delete

Add rule

Outbound rules

Type

All traffic

Protocol

All

Port range

All

Destination

C.

0.0.0.0/0

Description - optional

Delete

Add rule



You can add up to 50 more tags

Cancel

Create security group

Week- 5: Network Security in the Cloud





Step 6- Security Group Create Successfully.

 Security group (sg-0dffd052fd7ffc9 | security_group) was created successfully 

[▶ Details](#)

sg-0dffd052fd7ffc9 - security_group Actions ▼






Details

| | | | |
|--|--|--|---|
| Security group name  security_group | Security group ID  sg-0dffd052fd7ffc9 | Description  first security group | VPC ID  vpc-0b963cf2f9cf92e16 |
| Owner  355433852359 | Inbound rules count 1 Permission entry | Outbound rules count 1 Permission entry | |


Step 7- Block Unnecessary Ports, Edit Inbound and Outbound Rules


sg-0dffd052fd7ffc9 - security_group Actions ▼

Details

| | | | |
|--|--|--|--|
| Security group name  security_group | Security group ID  sg-0dffd052fd7ffc9 | Description  first security group | VPC ID  vpc-0b963cf2f9cf92e16 |
| Owner  355433852359 | Inbound rules count 1 Permission entry | Outbound rules count 1 Permission entry | |

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#)

Inbound rules (1)  [Manage tags](#) [Edit inbound rules](#)

< 1 > 

| <input type="checkbox"/> | Name ▼ | Security group rule ID ▼ | IP version ▼ | Type |
|--------------------------|--------|--------------------------|--------------|------|
| <input type="checkbox"/> | - | sgr-0828b72ffd224e2a0 | IPv4 | SSH |

Week- 5: Network Security in the Cloud

EC2 > Security Groups > sg-0dffd052fd7ffc9 - security_group > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

| Security group rule ID | Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Source <small>Info</small> | Description - optional <small>Info</small> | |
|------------------------|--------------------------|------------------------------|--------------------------------|--|--|--------|
| sg-0828b72ffd224e2a0 | SSH | TCP | 22 | C. <input type="text" value="47.11.10.18/32"/> | | Delete |

Add rule

Cancel Preview changes Save rules

aws [Alt+S]

EC2 > Security Groups > sg-0dffd052fd7ffc9 - security_group > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

| Security group rule ID | Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Source <small>Info</small> | Description - optional <small>Info</small> | |
|------------------------|--------------------------|------------------------------|--------------------------------|--|--|--------|
| sg-0828b72ffd224e2a0 | SSH | TCP | 22 | C. <input type="text" value="47.11.10.18/32"/> | | Delete |

Add rule

Cancel Preview changes Save rules

Step 8- Unnecessary ports are now blocked and your instance is more secure.

Step 9-

| Direction | Port | Protocol | Source/Destination | Description |
|-----------|------|----------|--------------------|----------------|
| Inbound | 20 | TCP | My IP | SSH for admin |
| Inbound | 80 | TCP | Anywhere | HTTP for web |
| Outbound | All | All | 0.0.0.0/0 | Default method |